FortiManager - Best Practices

FORTINET DOCUMENT LIBRARY
http://docs.fortinet.com

FORTINET VIDEO GUIDE
http://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTIGATE COOKBOOK
http://cookbook.fortinet.com

FORTINET TRAINING SERVICES
http://www.fortinet.com/training

FORTIGUARD CENTER
http://www.fortiguard.com

END USER LICENSE AGREEMENT
http://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdocs@fortinet.com

January 18, 2018
FortiManager Best Practices
02-000-443993-20180118

TABLE OF CONTENTS

Change Log

Date	Change Description
2017-08-21	Initial release.
2017-10-05	Updated sections: • Replace managed device. • ADOM Design. • Normal versus Backup Mode.
2017-10-27	Added geographic redundancy information. Updated the security practices topic to include placing the FortiManager behind a firewall.
2017-11-22	Updated sections: • Back up the configuration: compare checksum to verify backup.
	Updated sections:
2018-01-18	Updated geographic redundancy information.

Overview

This guide is a collection of best practices guidelines for using FortiManager. Use these best practices to help you get the most out of your FortiManager products, maximize performance, and avoid potential problems.

Additional information

For product and feature guides, go to the Fortinet Document Library at http://docs.fortinet.com.

For procedures on how to implement these best practices, see the *FortiManager Administration Guide* in the Fortinet Document Library.

For customer service and support, go to https://support.fortinet.com.

For technical notes, how-to articles, FAQs, and links to the technical forum and technical documentation, go to the Fortinet Knowledge Base at http://kb.fortinet.com/kb.

Installation

Plan your installation carefully and select the FortiManager model(s) that meet your requirements.

- Plan the size of your installation appropriately. Ensure you plan for future management and logging requirements, including consideration for:
  - The number of connected devices.
  - If applicable, log rates and analytic and archive retention periods.
- Ensure you have remote serial console or virtual console access.
- Ensure a local TFTP server is available on a network local to the FortiManager.

Business Continuity

- Ensure there is no power interruption. A power loss could cause the loss of a FortiManager device's database integrity. See Maintain database integrity on page 8.
  - Always shut down or reboot the FortiManager gracefully. Removing power without a graceful shutdown might damage FortiManager databases.
  - Ensure the FortiManager environment has a stable and uninterruptible power supply.
- If an unexpected power loss occurs, revert to a known good backup of the configuration.
- Ensure there are spare parts on site, such as fans, power supplies, and hard disk drives.
- Set up and use High Availability (HA).

Geographic redundancy

In order to increase resiliency, implement geographic redundancy when clustering FortiManager devices. That is, situate your FortiManager devices in locations that are not affected by the same conditions, such as power outages or floods.

In the event that the original primary FortiManager fails, the new primary FortiManager will attempt to contact all of the managed devices after the admin user has promoted the FortiManager to primary AND has issued the `exec fgfm reclaim` command. If any of your managed devices are behind a NAT device, the new primary FortiManager may be unable to connect to the managed devices, depending on whether that NAT is 1-to-1. In the event that FortiManager is unable to initiate a connection to managed devices, you must manually repoint the managed devices to the new primary FortiManager since they only have the IP address for the previous primary FortiManager.

General Maintenance

Perform general maintenance tasks such as backup and restore so you can revert to a previous configuration if necessary.

Back up the configuration

- Perform regular backups to ensure you have a recent copy of your FortiManager configuration.
- Verify the backup by comparing the checksum in the log entry with that of the backed up file.
- Set up a backup schedule so you always have a recent backup of the configuration. See the *FortiManager CLI Reference*.
- If your FortiManager is a virtual machine, you can also use VM snapshots.

If you use ADOMs, a large number of ADOMs can significantly increase the size of configuration files which increases backup and restore time. See ADOM considerations on page 13.

Schedule maintenance tasks for off-peak hours

Fortinet recommends scheduling maintenance tasks for off-peak hours whenever possible, including tasks such as:

- Configuration backup.
- Log deletion (if FortiAnalyzer features are enabled).
- Log rolling and related log upload (if FortiAnalyzer features are enabled).

Maintain database integrity

To maintain database integrity, never power off a FortiManager unit without a graceful shutdown. Removing power without a proper shutdown can damage FortiManager databases.

Always use the following CLI command to shutdown the device before removing power:

```
execute shutdown
```

Fortinet highly recommends connecting FortiManager units to an uninterruptible power supply (UPS) to prevent unexpected power issues that might damage internal databases.

Replace managed device

When you replace a standalone FortiGate device, the usual and recommended method in FortiManager is to use `execute device replace sn`.

When you replace a FortiGate cluster member, you don't need to use `execute device replace sn` because the cluster updates FortiManager about the new cluster member.

If the new cluster member appears in FortiManager as unregistered, delete it from the unregistered device list so that FortiManager can discover the new device as a cluster member.

If the FortiAnalyzer feature set is used and you need to replace a standalone FortiGate device or a cluster member, the best practice is to add the new device as a new member so as to preserve existing logs. Consider adding the old and new FortiGate devices into a group for reporting purposes.

For information on replacing FortiGate units in a high-availability pair, see the cookbook recipe Replacing FortiGate HA Pairs with Logging Enabled.

Replace the FortiManager device

If the FortiAnalyzer feature set is enabled and you need to move logs to a new FortiManager device, use log aggregation. See http://cookbook.fortinet.com/fortianalyzer-log-data-migration-old-new-fortianalyzer/. If the FortiManager being replaced is the primary, after replacing it, use `execute fgfm reclaim-dev-tunnel` to force FortiGates to connect to the new FortiManager.

Configuration Management

If there is more than one admin account per ADOM, enable workspace - either normal or workflow to control concurrent operator usage. See Concurrent administrators on page 10.

Use FortiManager to make FortiGate changes, rather than making changes in the FortiGate GUI. If changes will by made in the FortiGate GUI, use *Backup Mode*. See Normal versus Backup Mode on page 10.

When importing policy packages:

- Be careful when handling object conflicts: Choosing the FortiGate value will override the FortiManager value and might affect other FortiGates in that ADOM. See What to do when an object conflict occurs on page 11.
- Include unused objects if you think you might use them in the future: FortiManager will remove unused objects on the FortiGate during the next install. Note that periodic cleanup of unused objects at the ADOM level is recommended. See What to do with unused objects on page 11.
- Download the Import Policy Report if you need a record of the import, including any changes made to objects to resolve object conflicts. See Import report on page 11.

When installing policy packages (see Installing policy packages on page 11):

- Each managed device should only have one policy package associated with it. This reduces the chances of administrative error when installing a policy package.
- When installing a policy package, review the *Install Preview* before completing the install.

Concurrent administrators

To prevent multiple administrators from making changes to the FortiManager database at the same time and causing conflicts, the workspace function should be enabled. This feature requires admin users to lock ADOMs and policy packages and/or objects before making changes to the database.

Normal versus Backup Mode

Once FortiGates are managed by a FortiManager that is operating in Normal Mode, whenever possible, configuration changes should be made on the FortiManager and not the FortiGate.

This is particularly true for changes to policies or objects that affect the *Policies & Objects* pane on the FortiManager. Any such changes made directly on a FortiGate will require manual changes to resynchronize the FortiManager with the FortiGate. Although the *Device Manager* pane will learn about the changes, these changes will be overridden by the next policy package installation, unless the ADOM level *Policy & Objects* have been updated.

If you intend to regularly make changes directly on the FortiGate, and only need FortiManager to act as a configuration repository, it is recommended that you use FortiManager in Backup Mode.

When FortiManager is in Normal Mode, GUI access to managed FortiGates is restricted to Read-Only mode in order to limit the number of changes made directly on the FortiGate. Super_User accounts have the option of switching to Read-Write mode.

Import policy

When using the *Add Device Wizard*, importing policies and related objects to the *Policies & Objects* level is the final step. Such an import can also be separately initiated for a device.

This step ensures that the ADOM database (*Policies & Objects* pane) is populated with the information needed for managing firewall policies on managed devices in that ADOM. It also helps to ensure that interface mapping is properly configured.

During the import, objects being imported may differ from objects of the same name that already exist in that ADOM database.

What to do when an object conflict occurs

The admin user must choose to either keep the FortiManager version of the conflicted object, or replace it with the FortiGate version.

If this is the first device that an import is being performed on in this ADOM, it is reasonable to choose the FortiGate version of the object if the syntax or value of this object is typical for other devices that will be imported.

If other devices have already been imported, choose the FortiManager version of the object so that existing managed devices are not negatively affected.

What to do with unused objects

By default, FortiManager will only import objects associated with the policies being imported. The admin user is given the opportunity to import objects not yet associated with policies.

If you anticipate using many of the unassociated objects in future policies, you can chose to import them. Note that importing unused objects will increase the size of the database.

Periodic cleanup of unused objects at the ADOM level is recommended.

Import report

Save a copy of the import report at the end of the import process. Otherwise, these details are not saved for reference purposes. An import policy report may be useful if contacting Fortinet technical support in the future.

Installing policy packages

Each policy package is intended to reflect the complete security policies for one or more managed FortiGates.

The following guidelines are intended to reduce the likelihood of administrative errors when installing configuration changes to FortiGates:

- Each managed device should only have one policy package associated with it. This will help to ensure that the wrong policy package is not mistakingly installed to a FortiGate.

- When installing a policy package, be sure to review the *Install Preview* before completing the installation. This is particularly important during the initial installation of a policy package to a FortiGate.

ADOM Design

Enable ADOMs to support devices other than FortiGates, upgrades of FortiGates not supported by ADOM migration, and upgrading policy package versions. See When to enable ADOMs on page 13.

When upgrading FortiGate versions, if possible, use the same ADOM. See Upgrading the firmware of managed devices on page 13.

Upgrade in the following order:

1. FortiGate.
2. ADOM.
3. Global (if used).

Before upgrading the FortiGate, confirm that the current FortiManager version is compatible with the new FortiGate version. If not, upgrade the FortiManager first.

ADOM revisions (see ADOM revisions on page 14):

- Use for significant changes.
- Implement a deletion policy to limit the number of retained revisions.

Periodically clean up unused objects. See What to do with unused objects on page 11.

For more information, see the *FortiManager Administration Guide*.

ADOM considerations

A large number of ADOMs can significantly increase the size of configuration files which increases backup and restore time. Do not create more ADOMs than your business needs.

When to enable ADOMs

By default, FortiManager manages all FortiGate devices in a common ADOM called the root ADOM.

Some reasons for enabling ADOMs are:

- Support for devices other than FortiGates.
- Organizing devices by administrative group, customer, or geographic location.

Upgrading the firmware of managed devices

Each ADOM has a firmware version associated with it. FortiGates must be running firmware in the same maintenance release to be added to the ADOM.

When you upgrade a FortiGate, it is not necessary to move it to a new ADOM, provided that ADOM upgrade is supported to the next FortiOS version level. Instead, you can upgrade the firmware of that FortiGate to the next higher maintenance release. Once all the FortiGates in an ADOM have been upgraded to the new maintenance release, you can upgrade the ADOM itself.

Using the ADOM upgrade option is recommended in most scenarios because it is much simpler than moving the devices to a new ADOM. Moving devices to a new ADOM requires importing policies for each moved device, and the creation of a new policy package in the new ADOM.

You might decide to move upgraded devices to a new ADOM if you are deploying new devices in the field anyway.

ADOM revisions

It is possible to keep a revision history of changes made at the policy and objects level. However, unlike at the device level, the revision history at this level can significantly increase the overall size of your configuration backup.

Guidelines for use of ADOM revision history:

- Use for significant changes only.
- Implement a deletion policy to limit the number of revisions retained.
- Using the install wizard does not automatically add an ADOM revision.

Log Management

Set up a log management strategy that gives a good balance of redundancy and performance. Retain logs log enough for business requirements and archive older logs for better performance.

This is only applicable when FortiAnalyzer features are enabled. See the *FortiManager Administration Guide* for details.

Set up a log backup strategy

- Set up a backup strategy for logs.
- Set up a schedule to roll and upload logs. You can use the GUI or CLI to set this up. For details, see the *System Settings > Device logs* section in the *FortiManager Administration Guide*.
  - You can also back up logs using the `execute backup logs` command. For details, see the *FortiManager CLI Reference*.

Set up redundancy

- For log storage redundancy, you can set this up at the disk level by selecting an appropriate RAID level.
- For log delivery redundancy, set FortiGates to send log to multiple devices, provided the FortiGate models support this function.

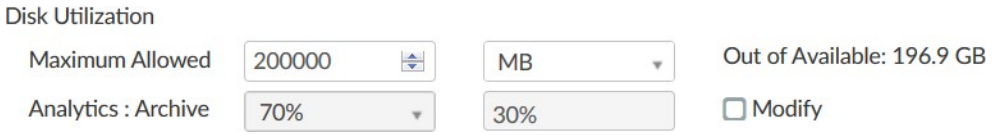
Set disk size and RAID level

Fortinet recommends using the default RAID level specified in the FortiManager data sheet, that is, RAID 50. If your configuration does not meet RAID 50 requirements, consider upgrading your hardware.

When planning for disk space requirements, consider future storage needs. Adding disks to an existing RAID array requires rebuilding the RAID array and restoring backed up logs.

The disk space available for you to set log quotas depends on the RAID level and the reserved space for temporary files. Temporary files are needed for indexing, reporting, and file management. In your planning, include both the disk space for the original logs FortiManager receives (Archive) and the space required to index the logs (Analytics).

Fortinet recommends using the default ratio of *Analytics : Archive* for most deployments. If you plan to retain archive logs for a much longer period than your analytical data, you might allocate a higher percentage to Archive.



If you need more disk space for a VM, add a virtual disk rather than change the size of an existing virtual disk. Use the `execute lvm extend` command to add a virtual disk. See the *FortiManager CLI Reference*.

Set log retention and storage

Determine the logs needed to meet business requirements

Consider carefully which types of logs to store on FortiManager. In some cases, you can be more selective about the type and volume of logs sent from FortiGate to FortiManager. Reducing the type and volume of logs gives FortiManager more resources to process the logs that meet your log storage, forensic, and reporting needs.

Allocate quota and set log retention policy

Ensure your quota settings is sufficient to fulfill your log retention policy. You must keep enough log data to meet your organization's reporting requirements. Configure quota settings and the log retention policy to ensure there is enough time to generate all scheduled reports.

Log View > *Storage Statistics* shows graphs with trends to help you with this planning.

If you are using ADOMs, ensure the quota is sufficient for every ADOM. Allocating insufficient quota to an ADOM might cause the following issues:

- Prevent you from meeting your log retention objective.
- Waste CPU resources enforcing quotas with log deletion and database trims.
- Adversely affect reporting when quota enforcement acts on analytical data before a report is complete.

For analytics, ensure the quota is sufficient and the retention period is long enough to complete all scheduled reports. When reports are generated and the log retention period is past, there is no need to keep analytical data since it can be regenerated from the original archived log data.

Use Fetcher Management for log fetching

To generate a report for a time period not covered by current analytical data:

- Use log fetching (*Fetcher Management*) to fetch archived logs to generate reports.
- Import log data from an external backup to generate reports.

Log fetching simplifies generating reports from log data for the following reasons:

- Log fetching allows you to specify the devices and time periods to be indexed.
- You can pull indexed logs into an ADOM with quota and log retention settings specifically set up to generate report on older logs.
- Log fetching helps to avoid duplications that might occur with importing data from an external backup.

For information on *Fetcher Management* (log fetching) and importing a log file, see the *FortiManager Administration Guide*.

Rebuild SQL database

Some firmware upgrades might change the SQL schema that indexes logs (analytics). If so, FortiManager automatically rebuilds the SQL database. During the rebuild, searching and reporting functions are limited.

You rarely need to manually rebuild an SQL database. If you think there might be problems with the SQL database, contact Customer Service & Support before considering a manual rebuild.

You might consider rebuilding the SQL database in the following situations:

- After moving a device to a new ADOM, you might need to rebuild the SQL database in the new ADOM.
- If disk space is running low, you might rebuild the SQL database to try free up disk space.

Report Performance

This is only applicable when FortiAnalyzer features are enabled. See the *FortiManager Administration Guide* for details.

For reports that you run regularly, set up the following:

- Put those reports into a group.
- Schedule those reports. If possible, schedule reports to run at off-peak hours and do not schedule reports to run at the same time as log maintenance tasks.
- Enable auto-cache for those reports.

If you regularly run a group of similar reports, put them into a group. Grouping reports can significantly improve performance and reduce report generation time. Grouping reports has these advantages:

- Reduce the number of *hcache* tables.
- Improve *auto-hcache* completion time.
- Improve report completion time.

Consider grouping reports in these conditions:

- If you use the same or a similar report template for different FortiGates.
- If you regularly use different filters on your reports.

Other ways to improve report performance include:

- Avoid running reports at the same time as log aggregation or log transfer.
- Avoid queries to external sources such as DNS (for name resolution) or LDAP (for obtaining a user list).

For more information, see the *FortiManager Administration Guide* and the *FortiAnalyzer Report Performance Troubleshooting Guide*.

Security Practices

For better security, implement the following:

- Use the proper encryption level. Use the SSL protocol version (TLS version) that meets PCI compliance or your organization's security requirements.

  For more information, see this knowledge base article: Setting SSL Protocol Version on FortiManager.
- Use two-factor authentication to improve log in security.
- Limit admin access, for example: trusted hosts, allowaccess, etc.
- Place the FortiManager behind a firewall, such as a FortiGate, to limit attempts to access the FortiManager device.

If the firewall in front of the FortiManager is NATing the traffic, configure the FortiManager with the dedicated public IP (see the Fortinet Knowledge Base article FD34605). This ensures that FortiGate devices are able to initiate communications (FGFM tunnels) to the FortiManager.

- For audit purposes:
  - Use named accounts wherever possible.
  - Send logs to a central log destination, like FortiAnalyzer.

Do not lose the administrator log in information as there is no password recovery mechanism in FortiManager 5.4.0 and later.

VM Size and License

When using VMs, implement the following:

- Allocate sufficient CPU and memory resources to all VMs.
- Ensure the VM license meets your requirements for daily log rate (GB/day) and log storage capacity.

For details, see the *FortiManager VM Install Guide*.